(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020020064469 A
(43)Date of publication of application: 09.08.2002

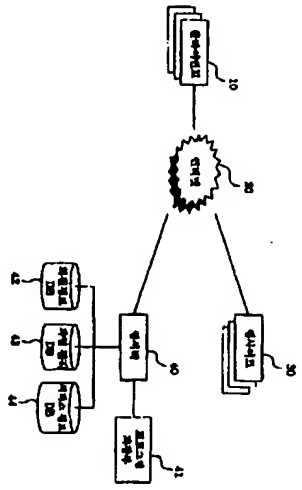
(21)Application number: 1020010004935
(22)Date of filing: 01.02.2001
(51)Int. Cl G06F 17/60

(71)Applicant: EVALI CORP.
(72)Inventor: KIM, YONG U

(54) METHOD AND SYSTEM FOR PROTECTING TRANSACTION CONTENTS BASED ON PUBLIC KEY USING INTERNET

(57) Abstract:

PURPOSE: A method and a system for protecting transaction contents based on the public key are provided to enable a user to protect transaction details on the Internet by executing a commodity purchase, a banking transaction, a stock transaction using the Internet and storing a coded transaction result screen in an additional recording medium through a non-public key.



CONSTITUTION: A user client(10) for making a user as an individual, a business entity, and a public office connect to the Internet(20) through a personal computer. The Internet(20) is a network for transmitting/receiving data through a communication in a remote place. A web site(30) as a bank, a security corporation, and a shopping mall is provided for supplying various real time electronic commerce services to a member user through the Internet(20). A web server(40) supplies a storing space capable of storing a result screen of transaction details in an additional recording medium to the user client(10) for making the user client(10) connect to the web site(30) through the Internet(20), receive a real time electronic commerce service, and protect transaction details.

Legal Status
Date of final disposal of an application (20031209)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G06F 17/60A2

(11) 공개번호 특2002-0064469
(43) 공개일자 2002년08월09일

(21) 출원번호 10-2001-0004935
(22) 출원일자 2001년02월01일

(71) 출원인 (주)한국전자증명원
서울특별시 강남구 역삼동 689-4번지 대웅빌딩 5층

(72) 발명자 김용우
서울특별시중구필동1가55-11번지

(74) 대리인 이철
이인실
염승윤

심사청구 : 있음

(54) 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스제공방법 및 시스템

요약

본 발명은 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템에 관한 것으로, 사용자가 전자거래 보호 서비스를 제공하는 웹사이트에 회원 가입하여 보관서비스 프로그램을 다운로드 받아 클라이언트에 설치하는 단계와; 사용자가 인터넷에 접속하여 전자거래를 실행하는 단계와; 사용자가 인터넷을 이용한 상기 전자거래의 거래내역 및 결과화면을 보관하기 위해 클라이언트에 설치된 보관서비스 프로그램을 구동시켜 보관 파일형식을 선택하여 보관 파일을 생성하는 단계와; 상기 보관서비스 프로그램은 생성된 보관 파일을 암호화 처리하고 해당 파일의 사용자 인증서를 이용하여 사용자 서명을 실행하는 단계와; 상기 사용자 서명이 완료되면 송신파일을 생성하여 인터넷을 통해 연결되는 전자거래 보호 서비스를 제공하는 웹서버로 전송 처리하는 단계와; 상기 회원 등록된 사용자들의 클라이언트로부터 송신자료가 수신되면 수신된 송신자료의 위/변조 여부를 검사하는 단계와; 상기 송신자료의 위/변조 검사결과 위/변조되지 않은 송신자료인 경우에는 송신자료에 포함된 사용자 인증서를 이용하여 사용자 확인 절차를 수행하는 단계와; 상기 송신자료의 사용자 신원이 확인된 경우에는 송신자료에 포함된 사용자 인증서를 통해 서명 확인 절차를 수행하는 단계와; 상기 송신자료의 사용자 서명이 확인된 경우에는 상기 전송된 송신자료의 정상수신 여부를 증명하기 위한 서명을 서버 인증서를 통해 실행하는 단계; 및 상기 송신자료를 해당 사용자에게 할당된 파일관리 데이터베이스에 저장하고 저장 확인문서를 해당 클라이언트로 전송 처리하는 단계를 포함하여 이루어진 것을 특징으로 한다.

따라서, 본 발명은 사용자가 인터넷을 이용하여 상품 구매나 은행 및 증권거래 등의 전자거래를 실행하고 결제내역 또는 거래 결과화면 등을 웹사이트 상의 기록매체에 비 공개키가 포함된 인증서를 통해서 암호화하여 저장함으로써, 인터넷상에서의 거래 내용을 보다 효과적으로 보호함은 물론 편리하게 보관할 수 있도록 된 것이다.

대표도
도 1

색인어
인터넷, 인증서, 공개키, 암호화, 파일관리, 보관, 보호, 검색, 위조, 변조

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템의 구성을 개략적으로 나타낸 블록구성도,

도 2 내지 도 5는 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법을 설명하기 위한 흐름도,

도 6은 본 발명에 따른 파일관리 데이터베이스의 데이터저장 화면상태를 나타낸 예시도.

♣ 도면의 주요부분에 대한 부호의 설명 ♣

10: 클라이언트 20: 인터넷

30: 웹사이트 40: 웹서버

41: 프로그램 저장부 42: 회원정보 데이터베이스(DB)

43: 파일관리 데이터베이스(DB) 44: 서비스정보 데이터베이스(DB)

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템에 관한 것으로, 보다 상세하게는 인터넷을 이용하여 물품 구매나 은행 및 증권거래 등을 실행하고 해당 거래내용의 결과화면을 별도의 기록매체에 저장함으로써, 인터넷상에서의 거래 내역을 보다 효과적으로 보호받을 수 있도록 된 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템에 관한 것이다.

현재, 지구상에는 인터넷을 기반으로 한 네트워크(Network)의 발달로 인하여 정보와 거래에 있어서 커다란 변혁을 맞이하고 있으며, 모든 정보를 공유하고 국경이 없이 거래하는 시대가 급속하게 다가오고 있다.

또한, 네트워크를 통한 가상공간의 창조는 이러한 가상공간 안에서의 각종 서비스 제공 및 온라인 실시간 거래를 불러일으키고 있으며, 이를 통한 오프라인의 실물거래 및 각종 대행서비스는 물론 온라인 상에서의 전문화된 정보 및 전자상거래 또한 활성화되고 있는 실정이다.

한편, 인터넷 사용자가 급속히 증가하면서 오프라인의 대형 매장, 은행, 증권사 및 유통회사 등이 인터넷을 이용한 온라인 실시간 서비스를 제공하고 있으며, 이러한 거래서비스의 사용 빈도수가 급증하고 있는 실정이다.

상기 인터넷을 이용하여 온라인 실시간 서비스를 제공받기 희망하는 사용자는 해당 웹사이트의 회원등록 절차를 통해 회원약관에 동의하고, 자신의 신상정보와 회원번호(ID) 및 비밀번호를 입력하게 되면 정식회원으로 등록되어 각종 실시간 거래 예컨대 증권거래, 은행거래 및 상품구입 등의 서비스를 제공받을 수 있게 된다.

발명이 이루고자 하는 기술적 과제

상기 인터넷을 이용하는 사용자가 상품을 구입하거나 은행 및 증권 거래를 실행한 후, 해당 대금을 결제하기 위하여 신용카드 또는 무통장 입금 처리하면 해당 웹사이트에서는 거래 내용의 결과화면을 화면으로 출력하여 표시하고, 사용자는 상기 화면을 인쇄 출력하여 보관하게 된다.

그러나, 상기 인터넷을 이용한 온라인 실시간 서비스는 네트워크인 인터넷을 통해서 이루어지고 있기 때문에 사용자의 거래 내용이 예컨대 전송에러, 통신장애 및 해킹에 의한 거래 내용 위/변조 등 여러 가지 장애요소로 인하여 사용자가 피해를 보는 사례가 증가하고 있어 새로운 사회문제로 확산되고 있다.

또한, 대다수의 사용자들이 상기 거래 내용의 결과화면을 인쇄 출력하지 않거나, 인쇄 출력하더라도 보관에 소홀하여 일정시간이 경과되면 해당 내용을 찾지 못하는 경우가 발생하여 상기 장애요소로 인한 사용자의 피해가 가중되고 있는 실정이다.

본 발명은 상기와 같은 문제를 해소하기 위한 것으로, 사용자가 인터넷을 이용하여 상품 구매나 은행 및 증권거래 등을 실행하고 거래 결과화면을 별도의 기록매체에 비 공개키를 통해 암호화하여 저장함으로써, 인터넷상에서의 거래 내역을 보다 효과적으로 보호받을 수 있도록 된 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

본 발명은 상기의 목적을 위하여, 사용자가 전자거래 보호 서비스를 제공하는 웹사이트에 회원 가입하여 보관서비스 프로그램을 다운로드 받아 클라이언트에 설치하는 단계와; 사용자가 인터넷에 접속하여 전자거래를 실행하는 단계와; 사용자가 인터넷을 이용한 상기 전자거래의 거래내역 및 결과화면을 보관하기 위해 클라이언트에 설치된 보관서비스 프로그램을 구동시켜 보관 파일형식을 선택하여 보관 파일을 생성하는 단계와; 상기 보관서비스 프로그램은 생성된 보관파일을 암호화 처리하고 해당 파일의 사용자 인증서를 이용하여 사용자 서명을 실행하는 단계와; 상기 사용자 서명이 완료되면 송신파일을 생성하여 인터넷을 통해 연결되는 전자거래 보호 서비스를 제공하는 웹서버로 전송 처리하는 단계와; 상기 회원 등록된 사용자들의 클라이언트로부터 송신자료가 수신되면 수신된 송신자료의 위/변조 여부를 검사하는 단계와; 상기 송신자료의 위/변조 검사결과 위/변조되지 않은 송신자료인 경우에는 송신자료에 포함된 사용자 인증서를 이용하여 사용자 확인 절차를 수행하는 단계와; 상기 송신자료의 사용자 신원이 확인된 경우에는 송신자료에 포함된 사용자 인증서를 통해 서명 확인 절차를 수행하는 단계와; 상기 송신자료의 사용자 서명이 확인된 경우에는 상기 전송된 송신자료의 정상수신 여부를 증명하기 위한 서명을 서버 인증서를 통해 실행하는 단계; 및 상기 송신자료를 해당 사용자에게 할당된 파일관리 데이터베이스에 저장하고 저장 확인문서를 해당 클라이언트로 전송 처리하는 단계를 포함하여 이루어진 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법을 제공한다.

본 발명의 다른 특징은 사용자가 개인용 컴퓨터를 통해 인터넷에 접속하기 위한 사용자 클라이언트와; 원격에서 통신을 통해 데이터를 송수신하기 위한 네트워크인 인터넷과; 상기 인터넷을 통해 회원으로 가입된 사용자들에게 소정의 실시간 전자거래 서비스를 제공하는 은행, 증권사 및 쇼핑몰 등의 웹사이트; 및 상기 클라이언트 사용자들이 인터넷을 통해 웹사이트에 접속하여 소정의 실시간 전자거래 서비스를 실행하고, 해당 거래내용을 보호받기 위하여 결과화면, 거래내역 및 문서파일 등을 보관파일로 선택하게 되면 회원 등록시 사용자에게 할당된 기록매체에 해당 보관파일을 저장하는 웹서버를 포함하여 구성된 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템을 제공한다.

이하, 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템을 첨부된 도면을 참조하여 상세하게 설명한다.

첨부된 도면, 도 1은 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템의 구성을 개략적으로 나타낸 블록구성도이고, 도 2 내지 도 5는 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법을 설명하기 위한 흐름도, 도 6은 본 발명에 따른 파일관리 데이터베이스의 데이터저장 화면상태를 나타낸 예시도이다.

이를 참조하면, 도 1에 도시된 바와 같이 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템은 개인, 기업체 및 관공서 등의 사용자가 개인용 컴퓨터를 통해 인터넷(20)에 접속하기 위한 사용자 클라이언트(10)와; 원격에서 통신을 통해 데이터를 송수신하기 위한 네트워크인 인터넷(20); 상기 인터넷(20)을 통해 회원으로 가입된 사용자들에게 다양한 실시간 전자거래 서비스를 제공하는 예컨대, 은행, 증권사 및 쇼핑몰 등의 웹사이트(30); 상기 클라이언트(10) 사용자들이 인터넷(20)을 통해 상기 웹사이트(30)에 접속하여 실시간 전자거래 서비스를 제공받고 거래 내용을 보호받기 위하여 거래내용의 결과화면을 별도의 기록매체에 저장할 수 있는 저장공간을 사용자들에게 제공하는 웹서버(40)로 구성되어 이루어진다.

상기 웹서버(40)는 회원으로 가입된 사용자들에게 제공되는 보관서비스 프로그램을 저장하는 프로그램 저장부(41)와, 회원 가입된 사용자들의 신상정보와 인증서 등을 저장하여 관리하는 회원정보 데이터베이스(42), 회원 가입된 사용자들의 인터넷을 통해 거래한 결과화면을 암호화하여 저장하고 사용자가 신청하는 일반파일을 암호화하여 저장하는 파일관리 데이터베이스(43), 전자거래 보호 웹사이트의 서비스 개요와 사이트 맵 등을 저장하는 서비스정보 데이터베이스(44)로 구성되어 이루어진다.

상기한 구성으로 된 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템의 동작을 도 2 내지 도 6을 참조하여 상세하게 설명한다.

상기 웹서버(40)를 운영하는 전자거래 보호 웹사이트 업체는 홈페이지를 통해 전자거래 보호 서비스에 대한 개요와 서비스 제공절차 등을 인터넷(20)을 통해 접속된 사용자들에게 안내 및 홍보하고, 회원으로 등록하는 사용자들에게 보호 서비스 프로그램을 무료 제공함과 더불어 인터넷 거래 결과화면 및 개인 파일 등을 저장할 수 있는 예컨대 30M의 저장공간을 무료로 제공하게 된다. 여기서, 사용자가 예컨대 30M 이상의 저장공간을 요구하는 경우에는 유료의 저장공간을 제공하게 된다.

상기 인터넷(20)을 이용하는 전자거래 보호 서비스를 제공받기 희망하는 일반 사용자가 자신의 클라이언트(10)에 설치된 웹브라우저를 실행하여 인터넷(20)에 접속한 후, 해당 웹사이트의 도메인을 주소창에 입력하게 되면, 상기 웹서버(40)는 서비스정보 데이터베이스(44)에 저장된 서비스 개요와 사이트 맵 등을 읽어들여 홈페이지를 통해 출력하게 된다(S11). 상기 홈페이지에는 웹사이트의 서비스 개요와, 서비스 절차 및 광고 등이 안내됨과 더불어 전자거래의 피해사례 및 대처 방안 등을 제시하여 회원 가입을 유도하게 된다.

사용자가 상기 홈페이지를 통해 제시된 회원 가입안내에 동의하여(S12) 회원가입을 선택하게 되면 상기 웹서버(40)는 사용자가 인증서를 소유하고 있는지 여부를 확인하게 된다(S13). 여기서, 상기 인증서는 인터넷(20)을 이용하는 사용자들이 전자서명법에 보호받을 수 있도록 공인인증기관(증권전산, 금융 결제원, 정보인증)으로부터 대면에 의해 발급되는 것으로, 발급된 공인 인증서에는 공개키 알고리즘이 포함되고, 사용자의 신원정보와 모두에게 공개하는 공개키와

사용자만이 확인 가능한 비 공개키로 구성된다.

상기 웹서버(40)는 사용자가 인증서를 소유하고 있지 않은 신규 회원인 경우에는 회원 신청서를 화면으로 출력하여 사용자에 의해 입력되는 신상정보 예컨대 회원번호(ID), 비밀번호, 주소, 연락처, 주거래 은행, 증권사 및 쇼핑몰 등을 회원정보 데이터베이스(42)에 등록 저장하게 된다(S14).

상기 웹서버(40)는 신규회원 사용자에게 해당 웹사이트에서 발행하는 인증서를 제공하고, 발생된 인증서를 회원정보 데이터베이스(42)에 저장함과 더불어 인터넷(20)을 이용한 전자거래 결과화면 및 일반파일을 보관할 수 있는 저장공간 사용 여부를 확인하여 희망하는 신규회원들에게 파일관리 데이터베이스(43)의 예컨대 30M 공간을 무료로 할당하게 된다. 여기서, 회원으로 가입된 사용자가 저장공간을 추가로 요구하는 경우에는 유료의 저장공간을 제공하게 된다.

상기 웹서버(40)는 인증서를 소유한 사용자에게 인증서 제출을 요구하고(S15), 사용자가 자신이 소지한 사용자 인증서를 제출하게 되면(S16) 해당 인증서를 회원정보 데이터베이스(42)에 저장한 후, 상기 프로그램 저장부(41)에 저장된 보관서비스 프로그램을 사용자의 클라이언트(10)로 다운로드 실행하여 다운로드가 완료되면 사용자는 자신의 클라이언트(10)인 개인용 컴퓨터에 보관서비스 프로그램를 설치하게 된다(S17).

상기 보관서비스 프로그램이 사용자 클라이언트(10)에 설치된 상태에서, 사용자가 인터넷(20)을 통해 온라인 실시간 서비스를 제공하는 예컨대 은행, 증권사 및 쇼핑몰 등의 웹사이트(30)에 접속하여 해당 웹사이트로부터 제공되는 전자상거래를 실행한 후, 해당 거래 결과화면을 보관하기 위하여 클라이언트(10)에 설치된 보관서비스 프로그램을 구동시키게 되면(S21), 도 3에 도시된 바와 같이 상기 보관서비스 프로그램은 사용자의 보관 파일형식을 결정하는 안내창을 화면으로 출력하여(S22) 상기 보관할 파일형식이 웹 페이지인지 여부를 판단하게 된다(S23).

상기 판단결과 보관할 파일형식이 웹 페이지인 경우에는 상기 보관서비스 프로그램은 사용자에 의해 선택되는 인터넷 전자거래 내용의 결과화면을 취득하여(S24) 보관 파일로 생성하게 된다(S25). 여기서, 상기 취득되는 웹 화면은 사용자가 인터넷(20)을 이용하여 전자거래의 행위가 발생한 웹브라우저의 화면을 취득하는 것으로, 사용자에 의해 웹 화면의 변조를 방지하기 위하여 화면에 표시된 자료의 제공 주소를 함께 취득하여 취득된 자료가 사용자에 의하여 변조됨을 방지하게 된다.

상기 판단결과 보관할 파일형식이 웹 페이지가 아닌 일반 문서파일인 경우에는 사용자가 해당 문서를 선택하도록 안내 메시지를 화면으로 출력하고, 사용자에 의해 선택되는 일반 파일을 보관 파일로 생성하게 된다(S26).

상기 보관서비스 프로그램은 보관할 파일이 생성되거나 선택된 경우에는 해당 파일을 암호화 처리하고(S27), 해당 파일의 사용자를 식별하기 위한 회원등록 시에 제출된 사용자의 인증서를 통해 사용자 서명을 실행하며(S28), 송신파일을 생성하여(S29) 인터넷(20)을 통해 연결되는 전자거래 보호 서비스를 제공하는 웹서버(40)로 전송 처리하게 된다(S30). 여기서, 상기 전송되는 송신파일은 전자서명법이 보호하는 공인인증기관의 인증서를 이용하여 사용자 자신이 해당 자료를 전송한다는 전자서명과 더불어 인증서와 함께 제공되는 타인에게 공개되지 않는 비 공개키를 이용하여 전송 자료에 전자서명(암호화 처리)을 하게 된다.

상기 인터넷(20)을 통해 전자거래 보호 서비스를 제공하는 웹서버(40)는 도 4에 도시된 바와 같이, 회원 등록된 사용자들의 클라이언트(10)로부터 송신자료가 수신되면(S51) 수신된 송신자료의 위/변조 여부를 검사하여(S52) 위/변조된 송신자료인 경우에는 해당 클라이언트(10)로 위/변조에 따른 전송에러 메시지를 전송하고 해당 프로세서를 종료하게 된다.

상기 송신자료의 위/변조 검사 방법은 사용자가 보관서비스 프로그램을 이용하여 전송하는 자료는 원본 문서와 원본 문서를 해쉬(Hash) 함수를 이용하여 취득한 해쉬 밸류(Hash Value)를 함께 전송하게 되는 바, 상기 웹서버(40)에서는 수신된 원본 문서를 해쉬 함수를 이용하여 새로이 해쉬 밸류를 취득하고, 사용자가 보내온 해쉬 밸류와 동일한 값인지를 비교하여 동일함 값인 경우에는 문서가 위/변조되지 않았음을 알 수 있게 된다. 여기서, 상기 해쉬 함수는 가변적인 어떠한 메시지를 처리하였을 때, 고정된 압축된 메시지 결과 값을 발생하고, 발생한 이 결과 값이 메시지에 따라 동일한 결과 값이 발생할 수 없으며, 결과 값으로부터 원본 메시지를 취득할 수 없는 기능을 가진 함수이다.

상기 웹서버(40)는 송신자료의 위/변조 검사결과, 위/변조되지 않은 경우에는 송신자료에 포함된 사용자 인증서를 이용하여 사용자 확인 절차를 수행하고(S54) 사용자의 신원이 인증서와 일치하는지 여부를 판단하여(S56) 일치하지 않은 경우에는 해당 클라이언트(10)로 신원확인 불일치에 따른 에러메시지를 전송하고 해당 프로세서를 종료하게 된다. 여기서, 상기 사용자 인증서가 공인인증기관으로부터 발급된 인증서인 경우에는 도시되지 않은 해당 공인인증기관과 인터넷(20)을 통해 접속하여 사용자의 신원을 확인하고, 상기 사용자 인증서가 전자거래 보호 서비스를 제공하는 웹사이트의 회원등록 시에 발급 받은 인증서인 경우에는 상기 회원정보 데이터베이스(42)에 저장된 사용자 인증서를 근거로 사용자 신원을 확인하게 된다.

상기 웹서버(40)는 송신자료의 사용자 신원이 확인된 경우에는 송신자료에 포함된 사용자 인증서를 통해 서명 확인 절차를 수행하고(S56) 사용자의 서명이 인증서와 일치하는지 여부를 판단하여(S57) 일치하지 않은 경우에는 해당 클라이언트(10)로 사용자 서명 불일치에 따른 에러메시지를 전송하고 해당 프로세서를 종료하게 된다. 여기서, 상기 사용자 서명을 확인하는 방법은 사용자가 타인에게 공개하지 않는 비 공개키로 암호화된 자료를 사용자의 인증서에 존재하는 공개키로 해독(검증작업)하여 사용자의 서명을 확인하게 된다.

상기 웹서버(40)는 송신자료의 사용자 서명이 확인된 경우에는 사용자가 전송한 송신자료를 정상적으로 받았다는 것을 증명하기 위한 서명을 서버 인증서로 실행하고(S58) 상기 송신자료를 해당 사용자에게 할당된 파일관리 데이터베이스(43)에 저장함과 더불어 저장 확인문서를 해당 클라이언트(10)로 전송 처리하게 된다(S59).

사용자가 자신의 보관 파일을 검색하기 위하여 도 5에 도시된 바와 같이, 인터넷(20)을 통해 전자거래 보호 서비스를 제공하는 웹사이트의 홈페이지에 접속하게 되면(S61), 상기 웹서버(40)는 사용자의 인증서 제출을 요구하고(S62) 사용자가 정상적으로 등록된 회원인 경우에는 도 6에 도시된 바와 같이 사용자 저장자료 검색창을 화면으로 출력하여 파일관리 데이터베이스(43)에 저장된 데이터의 리스트를 화면에 표시하게 된다(S63).

상기 웹서버(40)는 사용자가 화면으로 출력되는 소정의 검색자료를 선택하게 되면(S64) 해당 검색자료를 파일관리 데이터베이스(43)로부터 읽어들여 사용자 클라이언트로 다운로드 실행하게 된다(S45).

사용자는 자신의 클라이언트(10)에 다운로드된 보관자료를 보관서비스 프로그램을 통해 비 공개키를 이용하여 해당 보관자료의 암호를 해독함으로써, 해당 보관자료의 내용을 확인할 수 있게 된다.

이와 같이, 본 발명의 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템은 사용자가 인터넷을 이용하여 전자거래를 실행 한 후, 결제 내역 또는 거래 결과화면 등을 별도의 기록매체에 비 공개키가 포함된 인증서를 통해 암호화하여 저장함으로써, 인터넷상에서의 거래 내용을 보다 효과적으로 보호받을 수 있게 된다.

또한, 본 발명에 따른 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법 및 시스템은 단지 상기한 실시예에 한정되는 것이 아니고, 그 기술적 요지를 벗어나지 않는 범위에서 다양하게 변형 및 변경 실시할 수 있다.

발명의 효과

상술한 바와 같이, 본 발명에 의하면 사용자가 인터넷을 이용하여 상품 구매나 은행 및 증권거래 등의 전자거래를 실행하고 결제내역 또는 거래 결과화면 등을 웹사이트 상의 기록매체에 비 공개키가 포함된 인증서를 통해서 암호화하여 저장함으로써, 인터넷상에서의 거래 내용을 보다 효과적으로 보호함은 물론 편리하게 보관할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

사용자가 전자거래 보호 서비스를 제공하는 웹사이트에 회원 가입하여 보관서비스 프로그램을 다운로드 받아 클라이언트에 설치하는 단계와;

사용자가 인터넷에 접속하여 전자거래를 실행하는 단계와;

사용자가 인터넷을 이용한 상기 전자거래의 거래내역 및 결과화면을 보관하기 위해 클라이언트에 설치된 보관서비스 프로그램을 구동시켜 보관 파일형식을 선택하여 보관 파일을 생성하는 단계와;

상기 보관서비스 프로그램은 생성된 보관 파일을 암호화 처리하고 해당 파일의 사용자 인증서를 이용하여 사용자 서명을 실행하는 단계와;

상기 사용자 서명이 완료되면 송신파일을 생성하여 인터넷을 통해 연결되는 전자거래 보호 서비스를 제공하는 웹서버로 전송 처리하는 단계와;

상기 회원 등록된 사용자들의 클라이언트로부터 송신자료가 수신되면 수신된 송신자료의 위/변조 여부를 검사하는 단계와;

상기 송신자료의 위/변조 검사결과 위/변조되지 않은 송신자료인 경우에는 송신자료에 포함된 사용자 인증서를 이용하여 사용자 확인 절차를 수행하는 단계와;

상기 송신자료의 사용자 신원이 확인된 경우에는 송신자료에 포함된 사용자 인증서를 통해 서명 확인 절차를 수행하는 단계와;

상기 송신자료의 사용자 서명이 확인된 경우에는 상기 전송된 송신자료의 정상수신 여부를 증명하기 위한 서명을 서버 인증서를 통해 실행하는 단계와;

상기 송신자료를 해당 사용자에게 할당된 파일관리 데이터베이스에 저장하고 저장 확인문서를 해당 클라이언트로 전송처리하는 단계를 포함하여 이루어진 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 2.

제1항에 있어서,

상기 회원가입 절차는 사용자가 상기 웹사이트의 홈페이지를 통해 제시되는 회원약관에 동의하는 단계와; 사용자가 회원가입을 선택하게 되면 인증서를 소유하고 있는지 여부를 확인하고, 인증서를 소유한 사용자에게 인증서 제출을 요구하는 단계와; 사용자가 인증서를 소유하고 있지 않은 신규 회원인 경우에는 회원 신청서를 화면으로 출력하여 사용자에 의해 입력되는 신상정보와 사용자 인증서를 발행하여 회원정보 데이터베이스에 등록 저장하는 단계와; 인터넷을 이용한 전자거래 결과화면 및 일반파일을 보관할 수 있는 파일관리 데이터베이스의 저장공간을 할당하는 단계; 및 회원등록이 완료된 사용자에게는 보관서비스 프로그램을 사용자의 클라이언트로 다운로드 실행하는 단계를 포함하여 이루어진 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 3.

제1항 또는 제2항에 있어서,

상기 인증서는 인터넷 사용자들이 전자서명법에 보호받을 수 있도록 공인인증기관으로부터 대면에 의해 발급되는 것으로, 발급된 공인 인증서에는 공개키 알고리즘이 포함되고, 사용자의 신원정보와 모두에게 공개하는 공개키와 사용자만이 확인 가능한 비 공개키로 이루어진 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 4.

제1항에 있어서,

상기 보관 파일을 생성하는 단계에서, 상기 보관서비스 프로그램은 보관 파일형식을 결정하는 안내창을 화면으로 출력하여 사용자에 의해 선택되는 보관 파일형식이 웹 페이지인지 여부를 판단하는 단계와; 상기 판단결과 보관할 파일형식이 웹 페이지인 경우에는 사용자에 의해 선택되는 인터넷 전자거래 내용의 결과화면을 취득하여 보관 파일을 생성하는 단계; 및 상기 판단결과 보관할 파일형식이 일반 문서파일인 경우에는 사용자에 의해 선택된 일반 문서파일을 보관 파일로 생성하는 단계를 포함하여 이루어진 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 5.

제4항에 있어서,

상기 취득되는 웹 화면은 사용자가 인터넷을 이용하여 전자거래의 행위가 발생한 웹브라우저의 화면을 취득하는 것으로, 사용자에 의해 웹 화면의 변조를 방지하기 위하여 화면에 표시된 자료의 제공 주소를 함께 취득하는 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 6.

제1항에 있어서,

상기 송신자료의 위/변조 검사 방법은 사용자가 보관서비스 프로그램을 이용하여 전송하는 자료는 원본 문서와 원본문서를 해쉬 함수를 이용하여 취득한 해쉬 밸류를 함께 전송하고, 수신된 원본 문서를 해쉬 함수를 이용하여 새로이 해쉬 밸류를 취득함과 더불어 사용자가 보내온 해쉬 밸류와 동일한 값인지를 비교하여 문서의 위/변조 여부를 판단하는 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 7.

제1항 또는 제2항에 있어서,

상기 사용자 인증서가 공인인증기관으로부터 발급된 인증서인 경우에는 해당 공인인증기관과 인터넷을 통해 접속하여 사용자의 신원을 확인하고, 상기 사용자 인증서가 전자거래 보호 서비스를 제공하는 웹사이트의 회원등록 시에 발급 받은 인증서인 경우에는 상기 회원정보 데이터베이스에 저장된 사용자 인증서를 근거로 사용자 신원을 확인하는 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 8.

제1항에 있어서,

상기 사용자 서명을 확인하는 방법은 사용자가 타인에게 공개하지 않는 비 공개키로 암호화된 자료를 사용자의 인증서에 존재하는 공개키로 해독하여 사용자의 서명을 확인하는 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 9.

제1항에 있어서,

사용자가 자신의 보관 파일을 검색하기 위하여 인터넷을 통해 전자거래 보호 서비스를 제공하는 웹사이트의 홈페이지에 접속하는 단계와; 사용자의 인증서 제출을 요구하고 사용자가 정상적으로 등록된 회원인 경우에는 사용자 저장자료 검색창을 화면으로 출력하여 파일관리 데이터베이스에 저장된 데이터의 리스트를 화면에 표시하는 단계와; 사용자가 화면으로 출력되는 소정의 검색자료를 선택하게 되면 해당 검색자료를 파일관리 데이터베이스로부터 읽어들여 사용자 클라이언트로 다운로드 실행하는 단계; 및 사용자는 자신의 클라이언트에 다운로드된 보관자료를 보관서비스 프로그램을 통해 비 공개키를 이용하여 상기 보관자료의 암호를 해독하고 해당 보관자료를 확인하는 단계를 포함하여 이루어진 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 제공방법.

청구항 10.

사용자가 개인용 컴퓨터를 통해 인터넷(20)에 접속하기 위한 사용자 클라이언트(10)와;

원격에서 통신을 통해 데이터를 송수신하기 위한 네트워크인 인터넷(20)과;

상기 인터넷(20)을 통해 회원으로 가입된 사용자들에게 소정의 실시간 전자거래 서비스를 제공하는 은행, 증권사 및 쇼핑몰 등의 웹사이트(30); 및

상기 클라이언트(10) 사용자들이 인터넷(20)을 통해 웹사이트(30)에 접속하여 소정의 실시간 전자거래 서비스를 실행하고, 해당 거래내용을 보호받기 위하여 결과화면, 거래내역 및 문서파일 등을 보관파일로 선택하게 되면 회원 등록시 사용자에게 할당된 기록매체에 해당 보관파일을 저장하는 웹서버(40)를 포함하여 구성된 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템.

청구항 11.

제10항에 있어서,

상기 웹서버(40)는 회원으로 가입된 사용자들에게 제공되는 보관서비스 프로그램을 저장하는 프로그램 저장부(41)와;

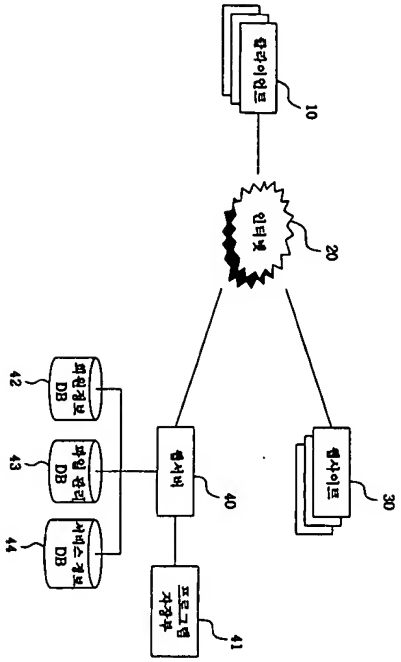
회원 가입된 사용자들의 신상정보와 인증서를 저장하여 관리하는 회원정보 데이터베이스(42)와;

회원 가입된 사용자들의 인터넷을 통해 거래한 거래내역 및 결과화면과 사용자가 신청한 일반 문서파일을 암호화하여 저장하는 파일관리 데이터베이스(43); 및

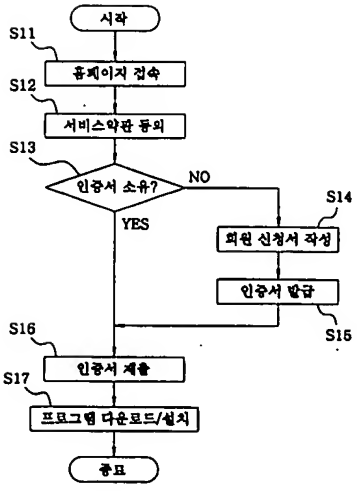
전자거래 보호 서비스를 제공하는 웹사이트의 서비스 개요와 사이트 맵 등을 저장하는 서비스정보 데이터베이스(44)를 포함하여 구성된 것을 특징으로 하는 인터넷을 이용한 공개키 기반구조 거래내용 보호 서비스 시스템.

도면

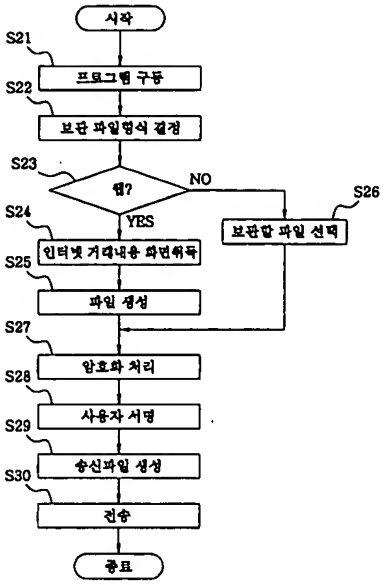
도면 1


클라이언트
10
인터넷
20
웹서버
40
솔루션
30
프로그램 다운로드
41
회원정보 DB
42
부가정보 DB
43
서비스정보 DB
44

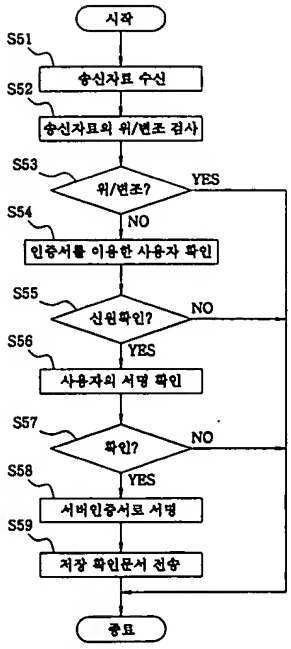
도면 2


시작
S11
홈페이지 접속
S12
서비스약관 동의
S13
인증서 소유?
NO
YES
S14
회원 신청서 작성
인증서 발급
S15
S16
인증서 제출
S17
프로그램 다운로드/설치
종료

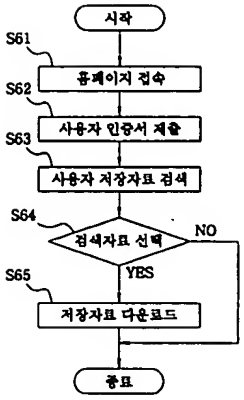
도면 3


시작
S21
프로그램 구동
S22
보관 파일형식 결정
S23
웹?
NO
S26
보관할 파일 선택
YES
S24
인터넷 거래내용 화면취득
S25
파일 생성
S27
암호화 처리
S28
사용자 서명
S29
송신파일 생성
S30
전송
종료

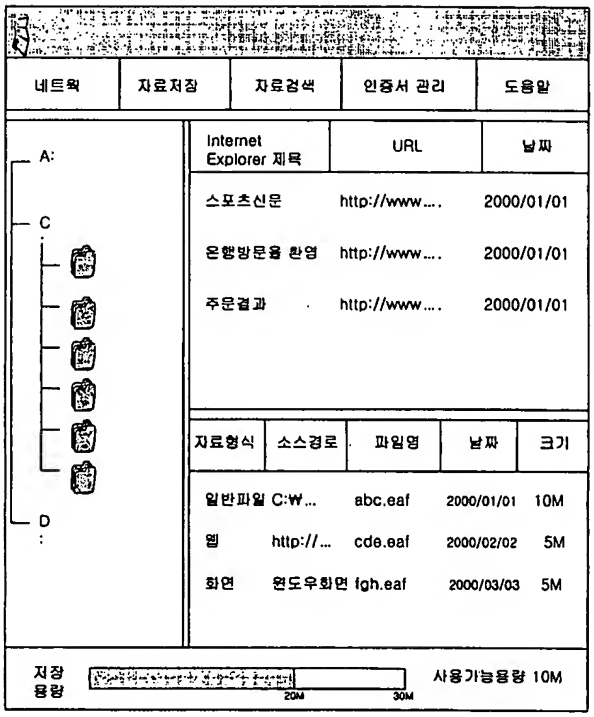
도면 4


시작
S51
송신자료 수신
S52
송신자료의 위/변조 검사
S53
위/변조?
YES
NO
S54
인증서를 이용한 사용자 확인
S55
신원확인?
NO
YES
S56
사용자의 서명 확인
S57
확인?
NO
YES
S58
서버인증서로 서명
S59
저장 확인문서 전송
종료

도면 5


시작
S61
웹페이지 접속
S62
사용자 인증서 제출
S63
사용자 저장자료 검색
S64
검색자료 선택
NO
YES
S65
저장자료 다운로드
종료

도면 6


네트웍
자료저장
자료검색
인증서 관리
도움말
A:
C
D
Internet Explorer 제목
URL
날짜
스포츠신문
http://www....
2000/01/01
은행방문을 환영
http://www....
2000/01/01
주문결과
http://www....
2000/01/01
자료형식
소스경로
파일명
날짜
크기
일반파일
C:₩...
abc.eaf
2000/01/01
10M
웹
http://...
cde.eaf
2000/02/02
5M
화면
윈도우화면
fgh.eaf
2000/03/03
5M
저장 용량
20M
30M
사용가능용량 10M